



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,728	11/07/2000	Patrick Le Quere	T2147-906625	8212
181 7590 08/24/2007 MILES & STOCKBRIDGE PC 1751 PINNACLE DRIVE SUITE 500 MCLEAN, VA 22102-3833			EXAMINER COLIN, CARL G	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 08/24/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/706,728

Applicant(s)

LE QUERE, PATRICK

Examiner

Carl Colin

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 May 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 15-18 and 20-34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 15-18 and 20-34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. In response to Pre-Appeal brief filed on 5/24/2007, the finality of the last Office Action has been withdrawn. The After Final amendment filed on 4/23/2007 has been entered. Applicant has amended claim 15. The following claims 15-18 and 20-34 are pending and are presented for examination.

Applicant's arguments in the Pre-Appeal brief filed on 5/24/2007 have been considered. Applicant's argument that Dyke does not disclose an Input/Output module comprising a microcontroller and memory that includes a flash memory and static memory is persuasive. However, claim 15 has been amended and no longer recites an input/output module that includes a flash memory and static memory. These features are disclosed in claim 29, which is rejected in view of Bakhle which has not been argued by Applicant. Upon further consideration, a new ground of rejection is set forth below.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to

Art Unit: 2136

which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 15-17 and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,604,683 to **Russ et al** in view of US Patent 6,021,201 to **Bakhle et al**.

As per claim 15, **Russ et al** substantially discloses an encryption circuit (1) for simultaneously processing various encryption algorithms, the encryption circuit adapted to be coupled with a host computer system, the encryption circuit comprising: a C-Bus module comprising elements 50, 51, 52, 54, and 56 (see column 4, lines 52-65) that meets the recitation of input/output module the C-Bus is connected to the Unibus of the host computer system via a dedicated bus as shown in fig.2 through element 56 (see column 9, lines 3-5) that meets the recitation of *an input/output module coupled to the host computer via a dedicated bus*. **Russ et al** discloses the C-bus is the primary controller and all the bus segments are dependent upon the control of the C-Bus (see column 7, line 50 through column 8, line 11) and including handling data exchanges between the host and the encryption unit (D-bus) (see column 11, lines 37-62) that meets the recitation of *the input/output module handles data exchanges between the host system and the encryption circuit*; the input/output module including a microprocessor and memory (see column 4, lines 52-58) that meets the recitation of *the input/output module including a microcontroller and memory*, **Russ et al** discloses an encryption module (DBUS) coupled with the input/output module (CBUS) (see figure 2); said encryption module controlling encryption and decryption operations, as well as storage of all sensitive information of the

Art Unit: 2136

encryption circuit (see column 9, lines 25-60); **Russ et al** discloses a RAM configured for isolation means operatively connected between the input/output module and the encryption module, the isolation means configured to make the sensitive information inaccessible to the host computer system (see column 2, lines 35-43).

Russ et al is silent about sensitive information stored in the encryption module. **Bakhle et al** in an analogous art discloses an input/output module including a microcontroller and memory (see figure 1), a dual-port memory and including a separate internal second bus isolated from the first bus of the dual-port memory, performing parallel processing of different cryptographic operations for example (see column 5, lines 14-67 and see figure 3); and the encryption circuit comprises a key storage unit for storing sensitive information (see column 6, lines 5-27). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption circuit of **Russ et al** to provide storage in the encryption module as taught by **Bakhle et al**. This modification would have been obvious because one of ordinary skill in the art would have recognized the importance of securing keys for cryptographic operations by storing them in secure storage for the predictable result of preventing tampering while benefiting from the features of **Bakhle et al** for providing the capability of performing parallel processing of different cryptographic operations.

As per claim 16, the combined references disclose the claimed circuit of claim 15 and further discloses wherein the isolation means comprises a dual-port memory (see **Russ et al**, fig. 1).

As per claim 17, the combined references disclose the claimed circuit of claim 15 and further discloses a dual-port memory coupled with an input/output module and an encryption module performing parallel processing and a dual-port memory being coupled to a first bus and adapted to simultaneously handle the exchange of data, commands and statuses between the input/output and encryption modules and providing means of isolating the input/output module and the encryption module (see **Russ et al** column 2, lines 35-43 and **Bakhle et al**, column 9, lines 45-61).

As per claim 29, **Russ et al** substantially discloses wherein the microcontroller comprises an input/output processor and a PCI interface integrating DMA channels for executing the data transfers between the host system and the circuit (see column 3, lines 59-65; and column 4, lines 59-62 and column 9, lines 1-7). **Bakhle et al** discloses an encryption circuit wherein a microcontroller comprises: an input/output processor and a PCI interface and a flash memory; integrating DMA channels responsible for executing the data transfers between the host system and the circuit, for example (see column 4, lines 26-67 and column 5, lines 34-44);

a flash memory containing the code of the input/output processor and a PCI interface, integrating DMA channels responsible for executing the data transfers between the host system and the circuit, for example (see column 4, lines 26-67); a flash memory containing the code of the input/output processor, for example (see column 4, lines 38-42); and an SRAM memory that receives a copy of the contents of the flash memory upon startup of the input/output processor, for example (see column 4, lines 26-67). **Bakhle et al** discloses instructions in the memory subsystem for the processors and examples of memory devices and the like that can be

implemented with the I/O module, such examples include DRAM, ROM, VRAM and the like.

Claim 29 is rejected on the same rationale as the rejection of claim 15 above.

As per claims 30-31, the combined references disclose the claimed circuit of claim 15.

Bakhle et al discloses card reader that for communicating with the encryption circuit that meets the recitation of a serial link, which is independent of the dedicated PCI bus, said link adapted to be controlled by the encryption module, and further discloses communication link such as phone line for performing remote encryption operation and transmitting specific algorithm to be employed that meets the recitation of wherein the serial link allows downloading of proprietary algorithms into the first encryption sub-module for example (see **Bakhle et al**, column 12, line 48 through column 13, line 25). Therefore claims 30-31 are rejected on the same rationale as the rejection of claim 15 above.

As per claim 32, **Bakhle et al** discloses the limitation of including a card supporting the circuit (column 12, lines 47-65).

3. **Claims 18 and 20-28, and 33-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,604,683 to **Russ et al** in view of US Patent 6,021,201 to **Bakhle et al**. as applied to claims 15-17 and further in view of IBM Technical Disclosure Bulletin, Cryptographic Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5.

As per claims 18 and 20, both references disclose the claimed encryption circuit of claims 15-17. **Bakhle et al** further discloses an input/output module including a microcontroller and memory (see figure 1), a first encryption sub-module, dedicated to the processing of symmetric encryption algorithms and being coupled with the first bus of the dual port memory, for example (see column 5, lines 14-67 and figure 3); a second encryption sub-module, dedicated to the processing of asymmetric encryption algorithms and being coupled with a first bus of a dual-port memory and including a separate internal second bus isolated from the first bus of the dual-port memory, performing parallel processing for example (see column 5, lines 14-67 and see figure 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption circuit of **Russ et al** to provide a first encryption module and second encryption module for simultaneously performing various encryption algorithms (column 5, lines 14-67) as taught by **Bakhle et al**. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided by **Bakhle et al** to provide a cryptographic device capable of performing cryptographic operations in different formats and while one type of operation is being performed another type can be performed concurrently or in parallel, for instance one cipher processor can operate on data having a first size whereas another processor can operate on a second block size (column 5, lines 14-27 and column 1, lines 32-45).

Russ et al does not explicitly disclose a CMOS memory which is coupled with the dual-port memory (4) via the first bus of the dual-port memory containing the encryption keys, for example which is well known in the art. These elements are well known in the art in a security device and can be implemented by the invention disclosed in Dyke. IBM Technical

Art Unit: 2136

Disclosure Bulletin supports well known art by disclosing a single-chip microcontroller comprising flash memory, data RAM memory, and CMOS memory. This bulletin further uses a CMOS memory to store security keys because it has the advantage to make probing and examination more difficult in attempt of removal as the CMOS's is sensitive to light and static charge. In addition the RAMs could be backed with a battery when the system was unpowered. Therefore, it would have been obvious to one of ordinary skill in the art of computer security at the time the invention was made to modify the circuit of as combined above to provide a CMOS memory coupled with the dual-port memory via the first bus of the dual-port memory containing the encryption keys as taught in IBM Technical Disclosure Bulletin. This modification would have been obvious because one skilled in the art would have been motivated to do so in order to make probing and examination more difficult in attempt of removal and the other advantage would be that the RAMs could be backed with a battery when the system was unpowered.

As per claim 21, **Bakhle et al.** discloses the limitation of an encryption circuit characterized in that the first encryption sub-module comprises an encryption component coupled with the dual-port memory via the first bus of the memory, comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and in that the second encryption sub-module comprises at least two encryption processors, respectively dedicated to the processing of asymmetric encryption algorithms, coupled with the encryption module via the internal second bus of the second sub-module, for example (see column 5, lines 14-67 and see figures 3 and 6 with description); and discloses a control unit comprises a security unit that control input and output and use buses separating from

the dual port bus (see figures 3-6 with description and table 2, column 8; column 13, lines 10 et seq.) that meets the recitation of and a bus isolator for isolating the second bus from the first bus of the dual port memory. **Bakhle et al** discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). Therefore, claim 21 is rejected on the same rationale as the rejection of claim 18 above.

As per claims 22-23, and 25, **Bakhle et al.** discloses the limitation of an encryption circuit characterized in that one of the two encryption processors is of the CIP type, and in that the other of the two encryption processors is of the ACE type, for example (see column 5, lines 50-67). **Bakhle et al.** discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). Having both processors CIP type is a design choice. Therefore, these claims are rejected on the same rationale as the rejection of claim 18 above.

As per claims 24 and 26, **Bakhle et al.** does not explicitly disclose that one of the processors and the encryption component comprise a FPGA. **Bakhle et al.** discloses input output buffer arrays, for example (see column 9, lines 55 et seq.) and also discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). It is apparent to one skilled in the art that the units disclosed by **Bakhle et al.** can comprise

FPGA without departing from the spirit and scope of the invention as such unit and component are also well known in the art. Therefore, these claims are rejected on the same rationale as the rejection of claim 18 above.

As per claim 27, the combined references above disclose the claimed circuit of claim 26 and further discloses encryption circuit comprises of PROM and SRAM (see page 2 and the figure in IBM TDB). It is also a design choice as the functions and advantages of different types of memory are well known and within the skills of one of ordinary skill in the art.

As per claim 28, the combined references above disclose the claimed circuit of claim 21. security mechanisms adapted to trigger a reset mechanism of memory are well known as disclosed in cited patent to Dyke (see column 8, lines 25-32 and lines 63-67). IBM bulletin further uses a CMOS memory to store security keys. Therefore, claim 28 is rejected on the same rationale as the rejection of claim 18 above.

As per claims 33-34, **Bakhle et al** discloses the limitation of including a card supporting the circuit (column 12, lines 47-65).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses some of the well-known claimed features. See PTO-form 892.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


/C.C./

Carl Colin

Patent Examiner

August 18, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


8, 20, 07